IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA	
v.	CRIMINAL ACTION NO.
DAVID SHEMTOV,	1:21-CR-0123-JPB-CMS
Defendant.	

FINAL REPORT & RECOMMENDATION

This case is before the Court on Defendant David Shemtov's motion to suppress evidence seized pursuant to two search warrants. [Docs. 27, 30]. For the reasons discussed below, I will recommend that this motion be denied.

I. BACKGROUND

A. The First Warrant

On April 15, 2020, FBI Special Agent Stephen R. Ryskoski submitted an application and affidavit for a search warrant to Google for information associated with 33 email addresses ("the Email Accounts").[1] [Doc. 27-2]. In his affidavit, Special Agent Ryskoski provided facts showing that certain unknown individuals

[1] It was later determined that several of the email addresses derived from the same account. The search ultimately yielded information from 15 unique accounts. [Doc. 36 at 3; Doc. 27-3 at 8–9].

were using the Email Accounts to perpetrate a fraud on a company that manages and administers buybacks for Apple iPhones ("the Victim Company"). [Doc. 27-2 ¶ 4]. The affidavit stated that the scheme exploited a "loophole" in the Victim Company's processes. [*Id.* ¶ 5]. Special Agent Ryskoski explained the buyback process and the loophole as follows.

Customers seeking to sell back an Apple iPhone complete an online form describing the device model and the condition of the phone. Upon receiving the completed online form, the Victim Company mails the customer a box to ship the device back, and advises the customer that the device must be unlocked. [Doc. 27-2 ¶ 6]. After the device is unlocked and inspected, the Victim Company sends an email to the customer, providing the amount—payable in an Apple gift card—it is willing to pay the customer in exchange for the device. [*Id.* ¶ 7]. If the customer refuses the offer, the device is mailed back to the customer. If the customer accepts the offer, the Victim Company keeps the device and emails the customer a link to redeem the Apple gift card. The link to the gift card is sent to the email address provided by the customer on the online trade-in request form. [*Id.*].

According to the affidavit, in July 2019, the Victim Company learned of a loophole in its trade-in process. The problem occurred if a device was returned in the locked mode and was described on the trade-in form as being a more valuable

model than it actually was; when this occurred, the Victim Company would send the customer an Apple gift card based on the incorrect (higher value) model. [Doc. 27-2 ¶ 8]. For example, if a customer falsely claimed to be trading in an iPhone XS, but actually sent in a locked iPhone 6, the customer would receive an Apple gift card valued over $500 when the customer should have received a gift card for less than $100. [*Id.*].

The affidavit states that in or around October 2019, the Victim Company started receiving trade-in requests that exploited the loophole described above, using the Email Accounts. [Doc. 27-2 ¶ 10]. From October 2019 until January 2020, the Victim Company received approximately 1,440 online trade-in requests exploiting the loophole, all with common mailing addresses, and the affidavit provides specific facts relevant to each of the Email Accounts. [*Id.* ¶¶ 11, 12]. Of the approximately 1,440 trade-in requests connected to the Email Accounts, all of the devices were represented to be newer model devices than they actually were, and each device was sent in the locked mode. [*Id.* ¶ 15].

The affidavit states that of the 1,440 trade-in requests, more than one thousand were actually fulfilled. [Doc. 27-2 ¶ 16]. The Victim Company identified the loophole on January 19, 2020, and fixed it that same day. [*Id.*]. The remaining trade-in requests were finalized after January 19, 2020, and were flagged as being

part of the scheme. [*Id.*]. Of the fulfilled trade-in requests that were part of this scheme, the Victim Company provided Apple gift cards totaling approximately $549,360 for devices that were only worth approximately $73,241. [*Id.*]. Had the remaining unfulfilled trade-in requests been honored, the Victim Company would have provided Apple gift cards totaling approximately $239,805 for devices that were worth only approximately $17,351. [*Id.*].

On April 15, 2020, United States Magistrate Judge Russell G. Vineyard signed the warrant that Special Agent Ryskoski had presented, which was assigned number 1:20-mc-670 (the "First Warrant"). [Doc. 61-1]. The First Warrant included an Attachment A and an Attachment B. Attachment A identified the email accounts that law enforcement was allowed to search. [*Id.* at 3–4]. Attachment B identified the things that law enforcement was allowed to seize and was divided into two sections: (I) information to be disclosed by Google and (II) information to be seized by the Government. [*Id.* at 5–7]. Section I required Google to produce certain information related to each email account, including "the contents of all emails associated with the account." [*Id.* at 5]. Section II contained a number of provisions limiting what the Government was entitled to seize. First, Section II limited the Government to seizing information that constituted "fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire

fraud), [and] 1349 (attempt and conspiracy) relating to the scheme to defraud [the Victim Company] of Apple gift cards." [*Id.* at 6]. Second, this section limited the Government to seizing information relating to acts occurring "after July 1, 2019." [*Id.*]. Third, Section II listed seven categories of information the Government could seize, including "[r]ecords related to gift card payments and confirmations received," "[r]ecords related to communications between the account owners and [the Victim Company]," "[r]ecords related to the use of the Apple gift cards received from [the Victim Company]," "[e]vidence relating to how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation," "[e]vidence relating to the planning, execution, furtherance and/or concealment of the crimes under investigation," "[e]vidence relating to the email account owner's and other participants' state of mind as it relates to the crimes under investigation," and "[t]he identity of the person(s) who created or used the user ID." [*Id.* at 6–7].

B. The Second Warrant

Four months later, on August 17, 2020, Special Agent Ryskoski submitted an application and affidavit for another search warrant—this time for a single email account, dshem26@gmail.com. In his affidavit, Agent Ryskoski provided the same background facts as he had in his earlier affidavit, and provided additional facts

regarding the dshem26@gmail.com address, specifically that (1) several email addresses that were used to submit devices for trade-in as part of the scheme either communicated with this new email account or listed this new email address in their contacts; and (2) law enforcement learned that one of the shipping addresses used in connection with the scheme was a UPS Store mailbox whose application listed this new email address as the contact address. [Doc. 27-3 ¶ 4].

On August 18, 2020, United States Magistrate Judge Justin S. Anand signed the warrant that Special Agent Ryskoski had presented, which was assigned number 1:20-mc-1462 (the "Second Warrant"). [Doc. 61-2]. Like the First Warrant, the Second Warrant included an Attachment A that identified the account to be searched [*id.* at 3], and an Attachment B that was divided into two sections and contained the same limitations as the First Warrant [*id.* at 4–6].[2]

C. Shemtov's Motion to Suppress

In his motion, Shemtov argues that evidence obtained from both the First Warrant and the Second Warrant (collectively "the Warrants") should be suppressed

[2] Like the First Warrant, Section I of Attachment B of the Second Warrant required Google to produce "the contents of all emails associated with the account." [Doc. 61-1 at 5; Doc. 61-2 at 4]. But the Second Warrant also contained a date restriction in Section I: "The contents of all emails associated with the account dated **after July 1, 2019**." [Doc. 61-2 at 4 (emphasis in the original)].

because the Warrants lacked probable cause and sufficient particularity. [Doc. 30 at 2–7, 3 n.1, 5 n.3]. I will address these arguments in turn.

II. DISCUSSION

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. Here, Shemtov challenges both probable cause and particularity.

A. Probable Cause

With respect to probable cause, "the task of a reviewing court is not to conduct a de novo determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate judge's decision to issue the warrant." *United States v. Bushay*, 859 F. Supp. 2d 1335, 1379 (N.D. Ga. 2012) (citing *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984)). Probable cause to support a search warrant exists when the totality of the circumstances allows a conclusion that there is a fair probability of finding contraband or evidence at a particular location. *United States v. Brundidge*, 170 F.3d 1350, 1352 (11th Cir. 1999). The search warrant affidavit must "state facts sufficient to justify a conclusion that evidence or contraband will probably be found at the premises to be searched." *United States v. Martin*, 297 F.3d 1308, 1314 (11th Cir. 2002) (citation

omitted). "[T]he affidavit should establish a connection between the defendant and the residence to be searched and a link between the residence and any criminal activity." *Id.* (citation omitted). Issuing judges are to employ a practical, commonsense approach to the probable cause analysis and should avoid hyper-technical review of the legitimacy of search warrants:

> In attempting to ensure that search warrant affidavits comply with the Fourth Amendment's prohibition against unreasonable searches and seizures resultant from warrants issued without probable cause, the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit, there is a fair probability that contraband or evidence of a crime will be found in a particular place. Probable cause deals with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act. Courts reviewing the legitimacy of search warrants should not interpret supporting affidavits in a hypertechnical manner; rather, a realistic and commonsense approach should be employed so as to encourage recourse to the warrant process and to promote the high level of deference traditionally given to magistrates in their probable cause determinations.

United States v. Miller, 24 F.3d 1357, 1361 (11th Cir. 1994) (internal citations and quote marks omitted). Reviewing courts accord "great deference" to judicial determinations of probable cause to issue a search warrant. *United States v. Leon*, 468 U.S. 897, 914 (1984); *Martin*, 297 F.3d at 1317.

Here, Shemtov asserts that the Warrants are not supported by probable cause because the scheme described in the affidavits does not amount to a crime. [Doc. 30

at 3]. Shemtov argues that the affidavits proffered only a scheme to deceive, rather than a scheme to commit fraud. [*Id.*]. According to Shemtov, "under the affiant's description, the Magistrate Judge did not have a substantial basis to conclude that it was [a crime]." [*Id.* at 4]. In support of this argument, Shemtov relies upon *United States v. Takhalov*, 827 F.3d 1307 (11th Cir. 2016).

In making this argument, Shemtov is asking this Court to conduct a pretrial analysis as to the substance of the Government's case, which I will not do in connection with evaluating probable cause for a search warrant. Moreover, I have previously rejected a related *Takhalov*-based argument in my Report and Recommendation dated August 23, 2022 ("the R&R"), in which I recommended denying Shemtov's motion to dismiss. [Doc. 49 at 8–13]. I incorporate that analysis here.

It is clear that the affidavits in support of the Warrants contained ample facts to support a conclusion that the Email Accounts would contain evidence of violations of 18 U.S.C. §§ 1341 (mail fraud), 1343 (wire fraud), and 1349 (attempt and conspiracy) relating to the buy-back scheme. It was eminently reasonable for the judges to find probable cause to believe that evidence related to the enumerated offenses would be found in the targeted email accounts based on the facts contained in the affidavits. Those facts describe a scheme where the fraudsters would

intentionally lie about the characteristics of the phones and deliberately return the phones in the locked mode in order to exploit the loophole and defraud the Victim Company of hundreds of thousands of dollars. Common sense dictates that the blatant misrepresentations about the device models accompanied by the submission of the misrepresented devices in the locked mode was an intentional effort to exploit the loophole and defraud the Victim Company. [Doc. 27-2 ¶ 8(f); Doc. 27-3 ¶ 8(f)]. The "totality of the circumstances" described in the affidavits established probable cause to believe that such evidence of the scheme would be found in the various Google email accounts, and that is all the law requires. *Brundidge*, 170 F.3d at 1352.

B. Particularity

Shemtov next argues that the Warrants are Constitutionally infirm because they failed to describe with sufficient particularity the things to be seized. In making this argument, he takes issue with the Attachment B's to the Warrants, which authorized a two-step seizure of information. [Doc. 30 at 4].[3] The Warrants at issue in this case employed the well-recognized two-step procedure for email accounts. In each of the warrants, Section I of Attachment B authorized law enforcement to first seize the entire contents of the email account(s) (step one), and then Section II

[3] He also states in a conclusory fashion that Attachment A is vague, but he provides no facts, argument, or caselaw to support this statement. [Doc. 30 at 5].

required law enforcement to segregate out and seize only the subset of information that fell within the scope of the warrant (step two). Shemtov appears to challenge the validity of this process, claiming that it amounts to an impermissible general warrant. [Doc. 30 at 6].

As noted above, the Fourth Amendment requires that a warrant particularly describe both the place to be searched and the persons or things to be seized. U.S. CONST. amend. IV; *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000). The particularity requirement protects against "the use of general warrants as instruments of oppression." *Stanford v. Texas*, 379 U.S. 476, 482 (1965). "The requirement that warrants particularly describe the place to be searched and the things to be seized makes general searches under them impossible." *Travers*, 233 F.3d at 1329. The Eleventh Circuit instructs that the particularity requirement "be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit." *United States v. Wuagneux*, 683 F.2d 1343, 1349 (11th Cir. 1982) (citations omitted).

With respect to electronic information, Federal Rule of Criminal Procedure 41(e)(2)(B) allows for the initial seizure of electronically stored information, followed by a later, off-site search of electronic evidence:

> **Warrant Seeking Electronically Stored Information.** A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

FED. R. CRIM. P. 41(e)(2)(B). According to the Advisory Committee Notes, this subsection was intended to create a two-step process whereby "officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant." FED. R. CRIM. P. 41(e)(2) advisory committee's note to 2009 amendments.

Email accounts, computer hard drives, phones, and other repositories of electronically stored information covered by Rule 41(e)(2)(B) often contain an enormous volume of data. Thus, it is well-settled that a warrant that requires disclosure of the entire contents of an email account (or permits an imaging of an entire hard drive or phone) and then describes a subset of that information that will be subject to seizure after a later, off-site review is reasonable as long as its descriptors are sufficiently specific. *See United States v. Lee*, No. 1:14-cr-227-TCB-

2, 2015 WL 5667102, at *3, 8–10 (N.D. Ga. Sept. 25, 2015) (concluding that a search warrant similar to the one in this case was sufficiently particular and stating, "a warrant that requires disclosure of the entire contents of an email account and then describes a subset of that information that will be subject to seizure is reasonable"); *United States v. Soviravong*, No. 1:19-cr-146-AT-CMS, 2019 WL 7906186, at *6 (N.D. Ga. Dec. 2, 2019) ("By explicitly limiting the scope of what may be searched and seized to evidence of the crimes under investigation, the [warrant] was sufficiently particular to enable the searchers to reasonably ascertain and identify the documents and information authorized to be seized."), *adopted by* 2020 WL 709284 (N.D. Ga. Feb. 12, 2020); *see also United States v. Chrisley*, No. 1:19-cr-297-ELR-JSA, 2021 WL 7286226, at *6 (N.D. Ga. Aug. 31, 2021) (finding that two-step warrants are permissible and recommending that the Government include date restrictions), *adopted by* 2022 WL 225621 (N.D. Ga. Jan. 26, 2022). To the extent Shemtov complains that the step-one process of disclosing the entire contents of the Email Accounts is overbroad [Doc. 30 at 6], he ignores this law, and his argument fails.

Shemtov, however, also argues that even if the two-step procedure might be permissible in some cases, his case is different. He claims that the Government included in the Warrants the following three categories of information that he claims

are so broad that they subsume the other limitations: (1) evidence relating to how and when the email account was accessed or used to determine the geographic and chronological context; (2) evidence relating to the planning, execution, furtherance and/or concealment of the crimes under investigation; and (3) evidence relating to the email account owner's and other participants' state of mind as it relates to the crimes under investigation. According to Shemtov, other warrants that courts have approved of did not contain these three broad categories. [Doc. 30 at 6–7].

The problem with this argument is that the Warrants authorize seizure only of information that would constitute "fruits, contraband, evidence, and instrumentalities" of the specified crimes. [Doc. 61-1 at 6; Doc. 61-2 at 5–6]. The Warrants clearly explained that the specific scheme being investigated was the scheme to defraud the Victim Company of Apple gift cards. [*Id.*]. The seven categories of documents (including the three about which Shemtov complains) are merely examples of the types of information that may constitute such evidence. Shemtov asks the Court to view these three categories of information in a vacuum, but that is not what the law instructs. Reviewing judges are required to analyze warrants with "a practical margin of flexibility" and to evaluate the type of property to be seized. In my view, the description of the property to be seized was as specific as the circumstances and nature of activity under investigation permitted. *See*

Wuagneux, 683 F.2d at 1349. Contrary to Shemtov's view that these three categories of items transformed the otherwise valid warrant into a general warrant, I think that instead they appropriately provided additional guidance to the officers conducting the search.

C. Good Faith

Shemtov's motion to suppress is also due to be denied based on the good faith exception to the exclusionary rule articulated by the Supreme Court in *United States v. Leon*, 468 U.S. 897, 922 (1984). In *Leon*, the Supreme Court held that even if a search warrant is ultimately found to be unsupported by probable cause, the Fourth Amendment will not bar admission of evidence obtained by law enforcement officers if the officers were acting in reasonable reliance upon the search warrant. *See Martin*, 297 F.3d at 1313 (citing *Leon*, 468 U.S. at 922).[4] The Eleventh Circuit interpreted *Leon* as follows:

> The *Leon* good faith exception applies in all but four limited sets of circumstances [citation omitted]. The four sets of circumstances are as follows: (1) where "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth"; (2) "where the issuing magistrate wholly abandoned his judicial

[4] The Eleventh Circuit has held that the *Leon* good faith exception also applies to violations of the particularity requirement, *see United States v. Accardo*, 749 F.2d 1477, 1479–81 (11th Cir. 1985), and to searches conducted pursuant to an overly broad warrant, *see Travers*, 233 F.3d at 1330.

> role in the manner condemned in" *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 99 S. Ct. 2319, 60 L. Ed. 2d 920 (1979); (3) where the affidavit supporting the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) where, depending upon the circumstances of the particular case, a warrant is "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid."

Id.

Based on my analysis above, I disagree with Shemtov's premise that there was anything wrong with the Warrants to begin with. The attachments to the Warrants are like those that are routinely authorized in this district, and they particularize the place to be searched and the things to be seized. Moreover, Special Agent Ryskoski's affidavit set forth the offenses that were being investigated, detailed the background of the investigation, and explained the scheme to defraud, resulting in ample probable cause to believe that evidence of the crimes under investigation would be found in the Email Accounts. The Warrants, therefore, are facially valid, and the agents who executed them were justified in relying on them.

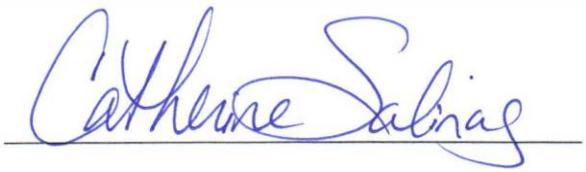
But even if the Warrants were invalid due to some issue of probable cause or particularity, the *Leon* good faith exception applies because the executing agents reasonably relied on the fact that Judges Vineyard and Anand signed the Warrants. Shemtov has not shown that any of the "four limited sets of circumstances" exists. Thus, even if the Warrant were Constitutionally infirm, the Fourth

Amendment does not bar admission of any evidence obtained pursuant to it. *See Blake*, 868 F.3d 960, 975 (11th Cir. 2017) (ruling that the *Leon* good faith exception to the exclusionary rule applied despite the lack of a temporal restriction, and noting: "[W]hile the warrants may have violated the particularity requirement, whether they did is not an open and shut matter; it is a close enough question that the warrants were not 'so facially deficient' that the FBI agents who executed them could not have reasonably believed them to be valid."). Here, neither of the Warrants was so facially deficient that the executing officers could not have reasonably presumed them to be valid. *Leon*, 468 U.S. at 923. For all the reasons stated, I find no basis for suppression.

IV. CONCLUSION

For the reasons stated, I **RECOMMEND** that Shemtov's motion to suppress [Docs. 27, 30] be **DENIED**. There are no other pending matters before me in this case. Accordingly, the case is hereby **CERTIFIED** ready for trial.

This 30th day of January, 2023.



CATHERINE M. SALINAS
United States Magistrate Judge